



Brief

LockBit Update: What Comes Next for the Extortion Collective?

B-2024-05-15a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Ransomware, Threat Actor

May 15, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on May 15, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | LockBit Update: What Comes Next for the Extortion Collective?

› Key Findings

- Increased pressure on LockBit's leadership following recent law enforcement (LE) activity is likely to make the extortion operation more volatile and unpredictable in the short term and may have negative consequences for extortion victims.
- LockBit's ability to persuade other ransomware and digital extortion (R&DE) threat actors that one of its operation's purported leadership figures, "LockBitSupp," was incorrectly identified and that its affiliates' identities remain secure is very likely hindered by recent reputational damage and degraded credibility.
- LockBit's inability to maintain stable infrastructure will likely be perceived by many threat actors as evidence that LockBit's operation is on a declining trajectory and is indicative of its leadership focusing on brand restoration rather than operational efficacy.
- Should barriers persist and hinder LockBit's ability to restore its reputation—as well as continued degradation in operational output—the likelihood that leadership will seek to close down LockBit's operation will increase.
- R&DE operations of this nature have a history of ceasing activity via exit scams conducted by the operations' leadership teams.

| Details

Increased pressure on LockBit's leadership resulting from recent LE activity is likely to make the extortion operation more volatile and unpredictable in the short term and may have negative consequences for extortion victims. LockBit's leadership is very likely at a crossroads with two options: continue attempting to restore credibility or close down the operation.

- LE's recent de-anonymization of leadership figure LockBitSupp likely exacerbates LockBit's existing difficulties in restoring its credibility in deep and dark web (DDW) communities.
- This increases the likelihood of the operation being closed down.

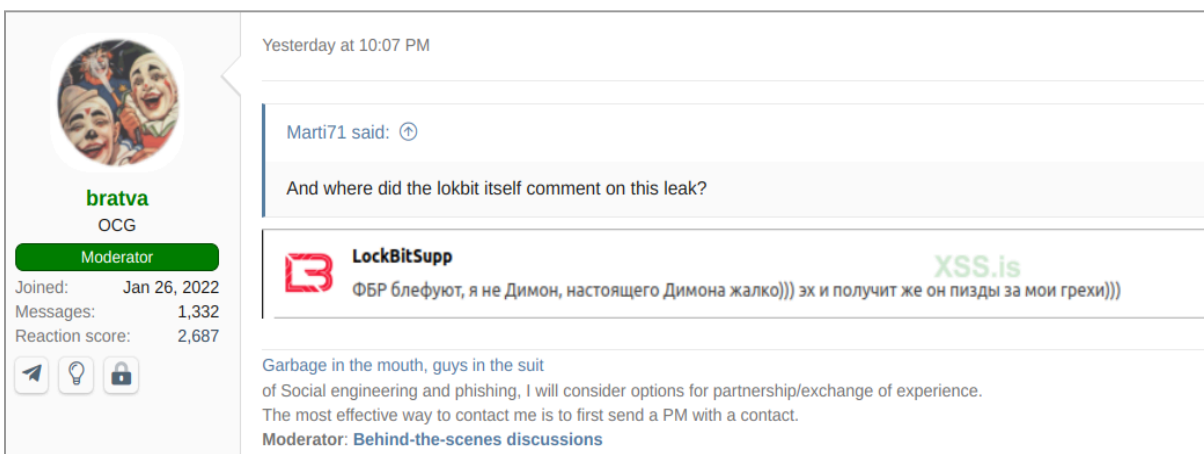
LE agencies published the alleged identity of LockBitSupp (referred to as "Dimon" in DDW communities) on May 7, 2024, claiming the alias is associated with Russian national Dmitry Yuryevich Khorosev. The de-anonymizing of LockBitSupp is very likely to be a second stage of Operation Cronos, a joint operation against LockBit between 11 LE agencies. Following the de-anonymization, Dmitry Yuryevich Khorosev was sanctioned by the United Kingdom, United States, and Australia, restricting victims' ability to make payments to LockBitSupp and making it increasingly difficult for anyone purportedly associated with them to elicit payments from victims in these regions.

- The first stage of Operation Cronos commenced on February 19, 2024. LE claimed to have seized LockBit's victim leaksites, affiliate panel source code, and victim information and released free decryption tools.
- While the operation had a short-term disruptive effect on LockBit's operations, it did not result in a sustained reduction in threat or the closure of the operation.
- LockBit's Ransomware-as-a-Service (RaaS) operation—which enables paying affiliates to carry out R&DE attacks—has been the most prolific R&DE operation for more than two years.

ZeroFox can neither independently confirm nor deny the identity of LockBitSupp as Dmitry Yuryevich Khorosev or whether the LockBitSupp moniker is operated by more than one individual. It is very likely that LockBitSupp and LockBit would refute the claims regardless of their veracity, seeking to maintain credibility and reassure present and future affiliates

that they are able to sufficiently protect their identities. Multiple individuals operating the LockBitSupp handle would almost certainly offer additional contingency in the event of a user being de-anonymized or subjected to LE scrutiny.

- LockBitSupp (via a TOX handle status) denied that Dmitry Yuryevich Khorosev was their identity and that the unconfirmed reveal achieved LE's very likely intended goals of disruption and reduction of credibility.
- LockBit posted subsequent denials on DDW forums xss and RAMP, implying that LE had doxxed an innocent Russian businessman.



Forum post denying the identity of LockBitSupp

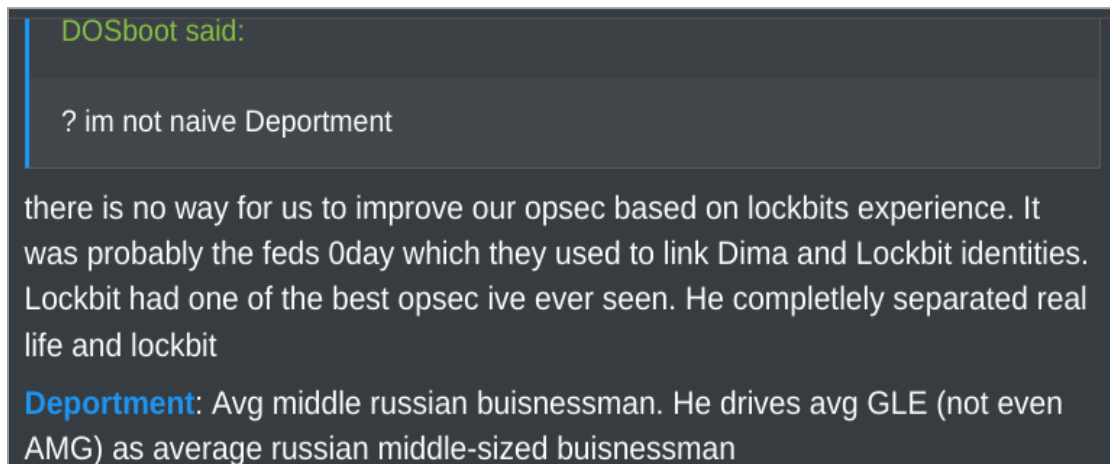
(Translation: "The FBI is bluffing, i'm not Dimon, too bad for the real Dimon, he'll suffer for my sins".)

Source: ZeroFox Intelligence

While endorsed by some DDW actors, LockBit's denials have failed to convince a substantial proportion of vocal actors in DDW communities, suggesting that an air of mistrust around the security of LockBit's operations—and the honesty of its leadership—prevails. Other threat actors, such as affiliates and likely other R&DE groups, have shown signs of being unmoved by the counterclaims, perceiving the LE-reported identity as true.

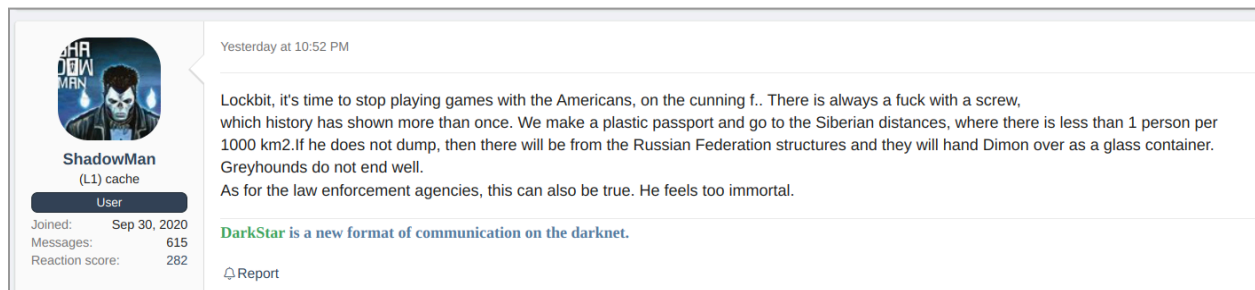
- In a RAMP thread, actor "Department" quoted multiple open-source intelligence investigations, implicitly confirming their belief in the identification of Dmitry Yuryevich Khorosev as LockBitSupp.

- Well-regarded actor “Shadowman” confirmed their belief in the identity of LockBitSupp. Furthermore, they stated that the correct identification opens up the possibility of the Russian Federation handing LockBitSupp over to the U.S. authorities.



Actor Department confirming their confidence in the identity of LockBitSupp

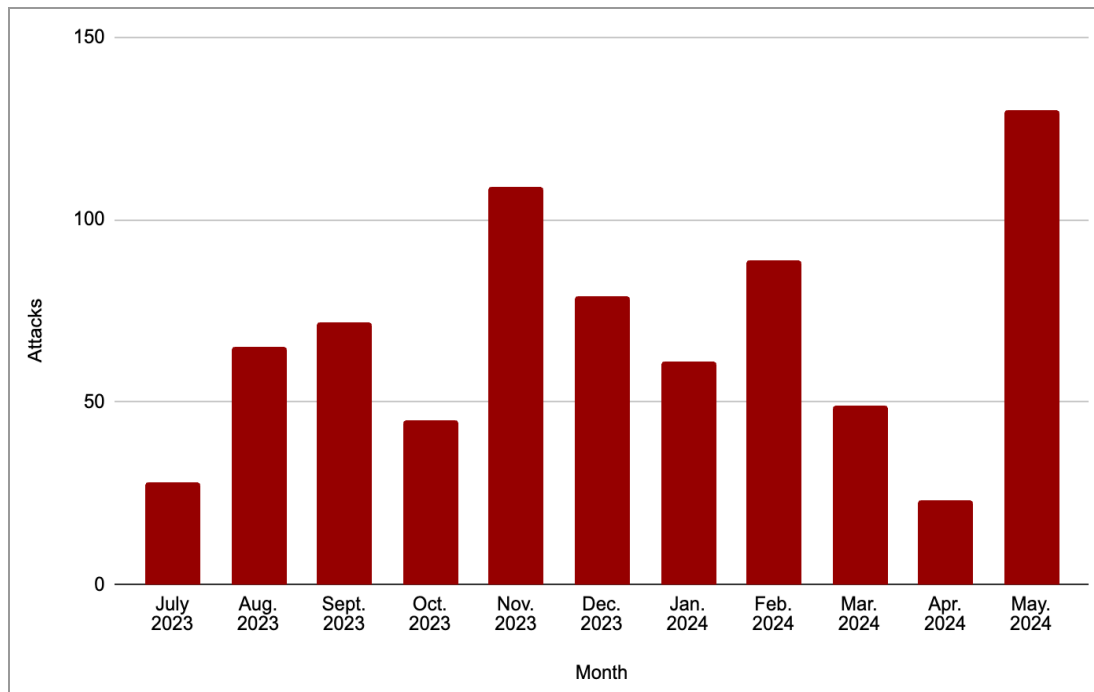
Source: ZeroFox Intelligence



Actor Shadowman confirming their confidence in the identity of LockBitSupp

Source: ZeroFox Intelligence

While LockBit remains operational, the group reported decreased numbers from its pre-LE disruption peak through April 2024. LockBit has listed at least 217 victims since the first stage of LE disruption on February 19, 2024; however, a notable increase in frequency has been observed so far in May 2024. These victims are very likely to include both recently targeted organizations, as well as those compromised prior to LE disruption. LockBit is very likely reposting old victims to give the perception that the organization is unaffected by recent events and garner increased confidence from affiliates.

**LockBit attacks by month***Source: ZeroFox Intelligence*

The challenges LockBit's leadership has faced to date in continuing its extortion operation post-Operation Cronos will likely increase in the coming weeks and months. LockBit's ability to persuade other R&DE threat actors that LockBitSupp was incorrectly identified and that its affiliates' identities remain secure is very likely hindered by recent reputational damage and degraded credibility. It is very likely in the interest of other R&DE collectives to promote LE's version of events, with the intention of discrediting LockBit and drawing experienced personnel from LockBit's operation.

LockBit's inability to maintain stable infrastructure will likely be perceived by many threat actors as evidence that LockBit's operation is on a declining trajectory, and it is indicative of its leadership focusing on brand restoration rather than operational efficacy. Tracked LockBit assets and infrastructure have been inaccessible for consecutive days on the DDW. Additionally, as of writing, no new victims have been released to LockBit's website for five consecutive days. This very likely suggests LockBit's infrastructure has been affected by recent LE activity. Continued downtime and unstable infrastructure will likely contribute towards affiliates gradually migrating to other RaaS groups.

- While LockBit's malware likely remains functional, continued LE disruption and the release of decryption software will likely impact the collective's long-term success.
- Operational instabilities may be perceived by extortionists as likely to impact negotiation channels and undermine trust that affiliates will be able to secure payment for their services.
- Repeated interruptions to infrastructure services will also likely impact LockBit leadership's ability to communicate with affiliates in a timely manner.

Sanctions placed on Dmitry Yuryevich Khorosev are very unlikely to be sufficient to eliminate ransom payments being made to LockBit. However, should there be complications—real or perceived—there is a roughly even chance that affiliates will be increasingly incentivized to deviate to other ransomware groups, diminishing LockBit's operational output.

- While LockBit's victims will very likely still be able to circumvent the sanction restrictions to make payments to LockBit, sanctions may be sufficient to deter some victims from paying.
- Additionally, sanctions will likely deter some threat actors from working with LockBit due to the perception there may be issues receiving payment or that LockBit affiliates may draw the attention of LE.
- ZeroFox has observed a significant drop in overall ransom payments in recent months. Any restrictions on LockBit that make eliciting payments even harder will likely drive affiliates to other RaaS operations that offer fewer barriers to obtaining payment.

The longer these barriers persist and hinder LockBit's ability to restore its reputation—alongside continued degradation in operational output—the more likely it becomes that leadership will seek to close down LockBit's operation. R&DE operations of this nature have a history of ceasing activity via exit scams conducted by the operations' leadership teams. Should LockBit choose to shut down, there is a roughly even chance that LockBit could conduct an exit scam using similar tactics as those employed by BlackCat (aka "ALPHV").

- LockBit has previously faced allegations of conducting exit scams against its affiliates, even as recently as March 2024. These claims have not been substantiated.

ALPHV / BlackCat Exit Scam (March 2024)

On March 3, 2024, RAMP member “notchy”, a self-proclaimed long-standing ALPHV affiliate, posted in the forum claiming that ALPHV’s leadership had scammed them out of a USD 20 million ransom payment made by a U.S.-based healthcare services provider. Notchy claimed the victim had made the payment to ALPHV’s “management” team, yet—despite notchy having conducted the attack and the negotiations—they were not paid.

ALPHV’s leadership had conducted an exit scam. They abruptly shut down their operations, ceasing contact and withholding all ransom payments made by victims without splitting the amount with affiliates.

This left the victim’s data in the hands of an unpaid ALPHV affiliate and the ransom in the hands of ALPHV’s leadership, meaning the affiliate had no incentive to return or delete the victim’s stolen data. The affiliate then approached another RaaS operation with the data, which extorted the same victim for a second time and was likely paid an additional ransom fee by the victim.

Aside from severing the relationship between core members and affiliates, LockBit conducting an exit scam would very likely have severe repercussions for ongoing extortion victims.

- An exit scam would very likely enhance the risk of victims being extorted multiple times for a single attack and increase the likelihood of ransom payments not guaranteeing the safety of the information and data stolen.
- In this case, ransom payments made to LockBit would not be shared with affiliates as agreed under the terms of the RaaS model. Instead, LockBit’s leadership would most likely run off with the payment.

- Affiliates who still hold victim data will very likely look elsewhere to ensure they receive payment for the stolen data. It is very likely that current and potential affiliates will seek to conduct their malicious activities under other operations.

Recommendations

- Leverage cyber threat intelligence to stay up to date on LockBit's activities and its operational capabilities.
- Ensure proactive detection of LockBit threats, their associated tactics, techniques, and procedures (TTPs), and Indicators of Compromise (IOCs).
- Develop a comprehensive incident response strategy, including the use of trusted third parties to assist with impact mitigation, communications, and ransom negotiations.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site or cloud servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system and ensure all business IT assets are updated with the latest software as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%